DENISE M. MINGRONE (STATE BAR NO. 135224)
dmingrone@orrick.com
ROBERT L. URIARTE (STATE BAR NO. 258274)
ruriarte@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025-1015
Telephone: +1 650 614 7400
Facsimile: +1 650 614 7401

CLAUDIA WILSON FROST (*Pro Hac Vice*)
cfrost@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
609 Main Street, 40th Floor
Houston, TX 77002-3106
Telephone: +1 713- 658 6460
Facsimile: +1 713 658 6401

Attorneys for Plaintiff and Counterdefendant,
SYNOPSYS, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

SYNOPSYS, INC.,

Plaintiff,

v.

UBIQUITI NETWORKS, INC., UBIQUITI NETWORKS INTERNATIONAL LIMITED, CHING-HAN TSAI, and DOES 1-20, inclusive,

Defendants.

UBIQUITI NETWORKS, INC.

Counterclaimant,

v.

SYNOPSYS, INC.,

Counterdefendant.

Case No. 3:17-cv-00561-WHO

THIRD AMENDED COMPLAINT FOR (1) VIOLATION OF DIGITAL MILLENNIUM COPYRIGHT ACT 17 U.S.C. § 1201(a)(1); (2) VIOLATION OF DIGITAL MILLENNIUM COPYRIGHT ACT 17 U.S.C. § 1201(a)(2); (3) VIOLATION OF DIGITAL MILLENNIUM COPYRIGHT ACT 17 U.S.C. § 1201(b); (4) VIOLATION OF 18 U.S.C. § 2318; (5) FRAUD; (6) CIVIL RICO, 18 U.S.C. § 1964; and (7) NEGLIGENT MISREPRESENTATION.

DEMAND FOR JURY TRIAL

Plaintiff Synopsys, Inc. ("Synopsys") hereby brings this Complaint against Defendants Ubiquiti Networks, Inc. ("Ubiquiti"), Ubiquiti Networks International, Ltd. ("UNIL"), and Ching-Han Tsai ("Tsai") for carrying out a coordinated software piracy scheme involving at least Synopsys' Debussy, Design Compiler, Formality, HSPICE, IC Compiler, Laker, Nlint, nWave, PrimeTime, Synplify Pro AV, Synplify Premier AV, TetraMAX, VCS, and Verdi applications, in violation of the Digital Millennium Copyright Act, 17 U.S.C. §§ 1201, *et seq*. (the "DMCA"), 18 U.S.C. § 2318 (relating to counterfeit and illicit documentation and labels), 18 U.S.C. § 1029 (relating to counterfeit access devices); 18 U.S.C § 1962 (relating to criminal enterprises); 17 U.S.C. § 506 & 18 U.S.C. § 2319 (relating to criminal copyright infringement); 18 U.S.C § 1343 (relating to wire fraud); 18 U.S.C. § 1512 (relating to obstruction of justice); and common law torts of deceit.

Synopsys seeks injunctive relief, statutory and/or actual damages, exemplary damages, attorneys' fees and costs, an accounting, and any such other relief as the Court may deem proper.

PARTIES

1. Plaintiff Synopsys is a corporation organized and existing under the laws of the State of Delaware, with its principal place of business in Mountain View, California.

2. Defendant Ubiquiti is a corporation organized and existing under the laws of the State of Delaware. Ubiquiti's principal place of business was 2580 Orchard Parkway, San Jose, California 95131 at the time this lawsuit commenced. Sometime during the summer of 2017, Ubiquiti moved its headquarters to 685 Third Avenue, 27th Floor New York, New York 10017. Ubiquiti continues to maintain a regular place of business in Pleasanton, California, within this judicial district.

3. According to Ubiquiti's February 9, 2017 10-Q filing with the U.S. Securities and Exchange Commission, Ubiquiti and its wholly owned subsidiaries develop high performance networking technology for service providers and enterprises.

4. According to Ubiquiti's February 9, 2017 10-Q, a significant portion of Ubiquiti's revenue is generated in the United States.

5. According to Ubiquiti's February 9, 2017 10-Q, certain of Ubiquiti's operating

expenses are denominated in the currencies of the countries in which its operations are located, including particularly the Taiwan Dollar. Significant parts of Ubiquiti's research and development operations are conducted outside the U.S., and Ubiquiti manages these geographically dispersed teams in order to meet its objectives for new product introduction, product quality, and product support.

6. UNIL is an entity incorporated under the laws of Hong Kong with a registered office address of 18/F Edinburgh Tower The Landmark 15 Queen's Road Central, Hong Kong. UNIL is a subsidiary of Ubiquiti and participates in Ubiquiti's activities relating to the development and distribution of networking technology. UNIL has a branch in Taiwan with a principal office at Suite 107, Floor 12, Song Ren Road, Xin Yi District, Taipei.

7. According to publicly available business information regarding UNIL, Robert J. Pera ("Pera") is a Director and the CEO of UNIL, and UNIL's business includes computer systems design services and exports. According to Ubiquiti's February 9, 2017 10-Q, Pera is also Ubiquiti's Chief Executive Officer, Chairman of the Board, founder, and Chief Operating Decision Maker. According to Ubiquiti's February 9, 2017 10-Q, Ubiquiti reports financial information on an aggregate and consolidated basis to Pera.

8. According to publicly available business information regarding UNIL, persons employed by UNIL's Taipei branch work in the field of semiconductor design, including the design of "IC's" or "integrated circuits" and "ASIC" or "application-specific integrated circuits."

9. Ubiquiti's SEC filings, publicly available information about UNIL and its employees, and representations made by Tsai and others to Synopsys indicate that, under Ubiquiti's management and direction, UNIL regularly conducts semiconductor design activities for Ubiquiti and designs products to be imported and sold in the United States, including in California. In addition, on information and belief, UNIL's company website is a subdomain of the "ubnt.com" web domain owned and controlled by Ubiquiti from California.

10. Defendant Tsai is an individual employed by Ubiquiti as a Project Lead. Tsai is a citizen of the United States who was domiciled in California during the inception of the scheme giving rise to this action.

11. Publicly available information published by Tsai indicates that he is a semiconductor professional with extensive experience in the design of integrated circuits, and that from October 2013 to present, Tsai has worked as a Project Lead for Ubiquiti, including in Taipei.

12. On information and belief, during the time period relevant to this action, Tsai regularly traveled to the United States and worked out of Ubiquiti facilities in California, including its former headquarters in the Northern District of California, and Ubiquiti's Barrington Illinois research facility.

13. Synopsys does not presently know the true names and capacities of the defendants sued herein as Does 1 through 20, inclusive. Synopsys will seek leave of court to amend this Complaint to allege said defendants' true names and capacities as soon as Synopsys ascertains them.

JURISDICTION AND VENUE

14. This action arises under the Digital Millennium Copyright Act, 17 U.S.C. §§ 1201, *et seq.*, 18 U.S.C. § 2318, 18 U.S.C § 1962, and California common law. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a).

15. This Court has personal jurisdiction over Ubiquiti because its principal place of business was located in the Northern District of California for the majority of the time period at issue in this case, because it continues to maintain a regular business address within the Northern District, and because it committed a substantial portion of the misconduct at issue in this case within the bounds of the Northern District, injuring Synopsys, who is also located in the Northern District. Ubiquiti has also submitted to the jurisdiction of this Court by filing a counterclaim against Synopsys.

16. This Court has personal jurisdiction over UNIL because UNIL expressly assented to personal jurisdiction in the Northern District of California for any disputes arising from UNIL's use of Synopsys' file download websites by affirmatively assenting to Synopsys' websites' terms of use in order to gain access to copyright-protected software and documentation hosted on Synopsys' file download website. *Inter alia*, one or more UNIL employees acting on

UNIL's behalf accessed Synopsys' SolvNet website on multiple dates subsequent to November 25, 2014, at which point Synopsys' terms of use provided in pertinent part: "These Terms govern your use of SolvNet and Content, in addition to the terms of the License Agreement…These Terms will be governed by and construed in accordance with the laws of the State of California, without regard to or application of conflict of laws rules or principles. You agree to submit to the exclusive jurisdiction of the courts located within the county of Santa Clara, California, to resolve any legal matter arising from these Terms." In order to access Synopsys' SolvNet website on or after November 25, 2014, it was necessary for a user to affirmatively assent to the terms of use by clicking a radio button that stated "YES, I AGREE TO THE ABOVE TERMS."

17. This Court also has personal jurisdiction over UNIL because UNIL committed a substantial part of the wrongful acts giving rise to this suit within California and the Northern District of California. *Inter alia*, UNIL knowingly and with the intent to make and distribute unauthorized copies downloaded software and documentation from Synopsys servers located in California and the Northern District, carried out business negotiations regarding the software at issue with Synopsys employees located in California, and Tsai, while physically present in California and acting on behalf of UNIL, misrepresented and omitted material facts to Synopsys in order to induce Synopsys to provide UNIL with access to Synopsys' copyright-protected software and documentation.

18. This Court also has personal jurisdiction over UNIL because of its regular business activities within and directed toward the State of California. Ubiquiti's SEC filings indicate that UNIL's semiconductor design activities are directed and funded from Ubiquiti's headquarters in the Northern District of California, and UNIL has an intimate and ongoing business relationship with Ubiquiti, Ubiquiti and UNIL CEO and board member Pera, and other Ubiquiti employees located in California, including Tsai, who regularly manage and direct UNIL's activities from within California and the Northern District of California. Ubiquiti personnel including Tsai have authority to negotiate, review, and approve licenses for semiconductor design software on behalf of UNIL, and UNIL requires such technology to perform its ordinary business activities. In addition, UNIL designs products for importation to and sale within the State of California,

including within the Northern District of California. UNIL has purposely availed itself of the laws of California by carrying out an ongoing business relationship with Ubiquiti in California, by purposely directing its normal business activities to California, and by filing a lawsuit as a plaintiff in at least one case in the Northern District of California.

19. This Court also has personal jurisdiction over UNIL because, contrary to Ubiquiti's and UNIL's repeated representations to this Court, discovery has revealed that UNIL employees traveled to California and the United States in furtherance of the violations of law alleged herein. In addition, UNIL employees involved in the wrongdoing at issue in this case signed employment agreements subjecting the employees and UNIL to California law and venue.

20. This Court has personal jurisdiction over Tsai because he owns real property in California, regularly conducted business in the State of California and Northern District of California, and committed a substantial part of the wrongful conduct at issue within the Northern District.

21. Venue in this district is appropriate under 28 U.S.C. §§ 1391 and 1400 because a substantial part of the events giving rise to the dispute occurred within this district.

FACTUAL ALLEGATIONS

General Background

22. As modern electronic devices become more and more compact and powerful, they use increasingly sophisticated computer processor chips. For example, computer chips found in modern networking equipment can contain millions of transistors. When designing a computer processing chip, the stakes are enormous. Chip designers need software that will ensure that their complex designs will work flawlessly. Accordingly, chip designers require extremely robust and powerful computer software to design and test those chips. Many of the world's biggest and most important chip design companies turn to Synopsys for that software.

23. Since it was founded in 1986, Synopsys has been a leading provider of Electronic Design Automation ("EDA") solutions for the semiconductor industry. EDA generally refers to using computers to design, verify, and simulate the performance of electronic circuits. For more than 30 years, Synopsys' solutions have helped semiconductor manufacturers and electronics

companies design, test, and manufacture microchips and electronic systems for a wide range of products. Headquartered in Mountain View, California, Synopsys is the fifteenth largest software company in the world and currently employs over 12,000 employees worldwide. Synopsys has developed a comprehensive, integrated portfolio of prototyping, IP, implementation, verification, manufacturing, optical, field-programmable gate array, and software quality and security solutions.

24. Synopsys' EDA software applications, including its Debussy, Design Compiler, Formality, HSPICE, IC Compiler, Laker, Nlint, nWave, PrimeTime, Synplify Pro AV, Synplify Premier AV, TetraMAX, VCS, and Verdi applications, are works subject to copyright protection under Title 17 of the United States Code.

25. Synopsys does not sell ownership rights or copyright or other intellectual property rights to its EDA software and associated services. Instead, Synopsys' customers purchase licenses. These licenses grant Synopsys customers limited rights to install Synopsys' EDA software and to access and use specific Synopsys software programs and documentation subject to control by Synopsys' License Key system.

26. Synopsys' License Key system is a built-in security system that controls access to its licensed software by requiring a user to access a key code provided by Synopsys in order to execute the licensed software. This key code controls the quantity and term of the licensed software in accordance with the license terms.

27. Neither Tsai, Ubiquiti, nor UNIL ever obtained a valid license from Synopsys to access and use the EDA software at issue herein. Instead, Tsai, Ubiquiti, and UNIL fraudulently induced Synopsys to grant them limited access to a subset of the Synopsys software for a finite evaluation period.

28. Since at least February 2014, Tsai, Ubiquiti, and UNIL have been secretly using counterfeit keys obtained and/or created with tools obtained through hacker websites to circumvent the Synopsys License Key system and access and use Synopsys' EDA software, including at least its Debussy, Design Compiler, Formality, HSPICE, IC Compiler, Laker, Nlint, nWave, PrimeTime, Synplify Pro AV, Synplify Premier AV, TetraMAX, VCS, and Verdi

applications, without a valid license. Tsai, Ubiquiti, and UNIL knew or had reason to know that their access and use of Synopsys' software was unauthorized and in violation of the DMCA and other U.S. laws designed to protect Synopsys' valuable intellectual property. The fact that they were not being required to pay Synopsys a license fee for access and use of the software alone should have put Tsai, Ubiquiti, and UNIL on notice that their access and use of Synopsys' software was unauthorized. Furthermore, use of counterfeit license keys continued even after Synopsys notified Ubiquiti of its unauthorized use of Synopsys' software—until at least December 2017, nearly a year after Synopsys filed the instant action. Defendants' corporate representatives have acknowledged under oath that Ubiquiti and UNIL employees knew they had no license to use Synopsys' software.

29. On information and belief, prior to October 2013, Tsai and others at Ubiquiti and UNIL conspired to, and did, form an associated in fact enterprise ("Piracy Enterprise") with a common purpose of pirating Synopsys' software in order to lower Ubiquiti and UNIL's semiconductor development costs and reap ill-gotten profits. Tsai, Ubiquiti, and UNIL each took wrongful acts in furtherance of their unlawful agreement by financing the Piracy Enterprise, attempting to gain and gaining unauthorized access to Synopsys' software and documentation, making and distributing unauthorized copies of Synopsys' software and documentation, using counterfeit and illicit license keys and counterfeit access devices to make unauthorized access to Synopsys' copyright-protected software, and obfuscating or destroying evidence of their illegal conduct, among other wrongful acts in furtherance of the Piracy Enterprise. Tsai, Ubiquiti, and UNIL continuously and effectively carried out the purpose of the Piracy Enterprise from at least October 2013 to March 2018, causing harm to Synopsys in the form of at least, but not limited to, misappropriation of valuable intellectual property, lost licensing revenue, and costs associated with remediating their conduct.

30. Ubiquiti and UNIL share certain information technology infrastructure including shared company communications networks, file repositories, email servers, IP addresses, and external and internal websites, including the web domain "www.ubnt.com," which is registered, hosted, and maintained in the United States, and its subdomain "tw.corp.ubnt.com," both of

which are associated with the misconduct alleged herein. Tsai, Ubiquiti, and UNIL made use of this shared IT infrastructure in conducting the Piracy Enterprise.

31. Tsai, Ubiquiti, and UNIL have each used Internet communications transmitted by means of wire in interstate and foreign commerce in the course of conducting the Piracy Enterprise.

32. The Piracy Enterprise and its agents, while connected to the Internet via domains, subdomains, and shared IT infrastructure controlled by Ubiquiti and UNIL, have used counterfeit keys to circumvent the Synopsys License Key access-control system at least 39,000 times using multiple computers and devices associated with Ubiquiti, UNIL, and others. On information and belief, Defendant Tsai has personally used counterfeit license keys to circumvent the Synopsys License Key access-control system at least 66 times.

33. In addition to using counterfeit license keys, the Piracy Enterprise has created and distributed amongst its members (i) unauthorized and counterfeit copies of Synopsys' software and documentation, (ii) technology and components thereof designed for the specific purpose of circumventing technological measures that effectively control access to Synopsys' works, (iii) counterfeit access devices; (iv) counterfeit license keys, and (v) illicit license keys. On information and belief, the Piracy Enterprise has employed Ubiquiti and UNIL's shared IT infrastructure in carrying out its illegal distribution of such materials and course of conduct.

Ubiquiti and UNIL's Corporate Governance and Culture

34. Ubiquiti operates with a flat reporting structure that relies on individual contributors or small development teams to develop, test, and obtain feedback for its products.

35. Ubiquiti development teams are supervised by team leads who report directly to Ubiquiti executives, managers, and/or directors, including Ubiquiti CEO Robert Pera.

36. UNIL also operates with a flat reporting structure. UNIL development teams report directly to UNIL executives, managers, and/or directors, including UNIL CEO, Director, and Chairman of the Board Robert Pera.

37. Ubiquiti employs a lean management structure. During the time period relevant to this action, Ubiquiti's executive-level operational leadership team has been comprised of only

some combination of the following executives: Ubiquiti's CEO, Chief Financial Officer (CFO), Chief Accounting Officer, Vice President of Legal Affairs, Vice President of Business Development, and Vice President of Global Vendor Management ("Ubiquiti Management"). Some of these same Ubiquiti executives also act as UNIL's executive-level operational leadership. UNIL has no executives on its own payroll.

38. Ubiquiti has acknowledged in its SEC filings that Ubiquiti's lean management structure creates risks regarding Ubiquiti's ability to manage its business, including risks related to Ubiquiti's ability to manage its operations abroad and in Taiwan specifically.

39. Ubiquiti and UNIL are purportedly governed by a Code of Business Conduct and Ethics. At all times relevant, various combinations of Ubiquiti's CEO, CFO, Vice President of Legal Affairs, and Audit Committee were responsible for enforcing the Code of Business Conduct and Ethics at Ubiquiti and UNIL.

40. Neither Ubiquiti nor UNIL provide any training to employees on the meaning and force of the Code of Business Conduct and Ethics, and the documents is not printed in any language other than English despite the fact that Ubiquiti has numerous employees with limited or no English language skills.

41. In or about November 2010, Ubiquiti's Board of Directors or a Committee of the Board of Directors passed a resolution designating Ubiquiti's CFO as the company's Designated Ethics Officer. The CFO's responsibilities as the Designated Ethics Officer included receiving and investigating reports of suspected violations of Ubiquiti's Code of Business Conduct and Ethics and reporting such suspected violations to Ubiquiti's Audit Committee. However, Ubiquiti lacked a CFO for certain periods of time between November 2010 and April 2013, and during those periods of time, Ubiquiti had no Designated Ethics Officer.

42. In or about April 2013, Ubiquiti's Board of Directors or a Committee of the Board of Directors passed a resolution designating Ubiquiti's Chief Compliance Officer (CCO) as the company's Designated Ethics Officer. But Ubiquiti never hired a CCO and thus has had no Designated Ethics Officer from April 2013 to present.

43. Due to lax internal controls, the lack of a Designated Ethics Officer, and a

corporate culture that rewards profits at the expense of ethics, Ubiquiti and UNIL never enforced its Code of Business Conduct and Ethics with respect to the conduct alleged in the complaint. Indeed, Pera and, on information and belief, other members of the Ubiquiti Management team, while paying lip service to corporate policies from time to time, turned a blind eye to severe violations of the Code of Business Conduct and Ethics in their quest to develop a proprietary application specific circuit (ASIC) developed and incorporated into a marketable product. This ASIC development project, referred to internally at Ubiquiti and UNIL as the AME Project, is a core pillar of Ubiquiti's market strategy and was a personal priority for Pera. Because time was of the essence to Ubiquiti and UNIL, Ubiquiti Management incentivized their employees with promises of bonuses and other rewards in exchange for an on-time delivery of the AME Project ASIC. As part of their bargain with Pera and the company, Tsai and his AME Project team members repeatedly violated the companies' purported ethics policies and were subsequently rewarded by Pera himself for doing so.

Ubiquiti and Tsai Gain Access to Synopsys' Intellectual Property

44. In 2013, Ubiquiti needed electronic design automation (EDA) software for the AME Project, referred to above. In particular, EDA software was critical for designing and testing the new chips Ubiquiti was developing in the AME Project for the new line of Ubiquiti products, including the Ubiquiti airFiber 5xHD, which Pera had represented to investors would be a significant factor in the company's long term success. Pera was particularly proud of and frequently touted to the market the importance and value of Ubiquiti's developing its own proprietary ASIC for a new line of Ubiquiti products.

45. In or about mid-2013, Pera contacted Tsai via LinkedIn to recruit Tsai to work on the AME Project. Pera and Tsai subsequently met in person at a Starbucks in San Jose to discuss the project. The AME Project was an object of, and was carried out by, the Piracy Enterprise.

46. Pera hired Defendant Tsai on August 25, 2013. On August 28, 2013, with the support of Ubiquiti and UNIL, Tsai and Pera began recruiting and hiring persons to work on the AME Project at Ubiquiti and UNIL. These persons were known to Tsai to have experience procuring, distributing, and using counterfeit license keys and hacked versions of EDA software.

47. In addition to hiring the engineers who acted on behalf of the Piracy Enterprise and carried out the scheme to pirate Synopsys' software, Pera met face to face with EDA software providers and negotiated the price to pay for the few "legal licenses" that Tsai described in his piracy plan (Para. 55 & 59, supra). Pera received regular weekly to bi-weekly status reports on the AME Project along with a select few other project leaders, and he was deeply involved in the day to day operations of the AME Project carried out by the Piracy Enterprise.

48. According to chat logs recovered in forensic discovery ordered by U.S. Magistrate Judge Beeler (but not collected by Defendants in the course of ordinary document production), on September 10, 2013, UNIL employee Ya-Chau Yang transferred to Tsai via the interstate wires a pirated copy of an EDA software binary file developed, owned, and licensed by a United States EDA software company ("Company A"). In chat sessions, Tsai and Yang referred to the binary as a "cracked" copy of the EDA software. The file name for the binary Yang transferred to Tsai included the name of a known source of pirated software.

49. The day after Yang transferred to Tsai the "cracked" version of EDA software belonging to Company A, on September 11, 2013, Tsai, acting on behalf of the Piracy Enterprise, communicated with Synopsys employees in Mountain View, California via email and represented that Ubiquiti was interested in licensing "at a minimum" Synopsys VCS and Verdi EDA software applications. Tsai also represented that Ubiquiti was interested in licensing a separate suite of Synopsys semiconductor designs. On or about September 12, Tsai met in person with Synopsys employees in San Jose and stated that Ubiquiti was also interested in licensing Synopsys' Design Compiler application. On or about this same date, Tsai represented to Synopsys that Ubiquiti planned to build up a semiconductor design team at Ubiquiti's U.S. headquarters, and that Synopsys was its number one choice. Tsai's statements on September 11 and 12 were designed to, and did, create the impression that Ubiquiti was interested in creating a significant business relationship with Synopsys that would lead to substantial revenue. As evidenced by the conduct discussed below, Tsai's statements on September 11 and September 12, 2013 were false when made, and Tsai never intended to create the relationship or license the software from Synopsys as represented. Instead, as described in the piracy plan referenced in paragraphs 83-103 below, Tsai

only intended to acquire a few "legal licenses" from an EDA vendor and pirate the rest of the software needed for the project

50. On September 16, 2013, Tsai and Yang communicated, over interstate wires via computers used in interstate commerce, about methods and technology that they could use to pirate EDA software, circumvent EDA software licensing controls, and obtain EDA software binaries.

51. On September 30, 2013, acting on behalf of the Piracy Enterprise, Tsai emailed Synopsys in Mountain View and represented that Ubiquiti was interested in taking a total of 21 licenses for Synopsys VCS, Verdi, Design Compiler, and Formality EDA applications during the period from November 2013 to June 2014. Tsai represented that Ubiquiti was interested in obtaining licenses for VCS and Verdi applications by November 2013, additional licenses for these two products and Design Compiler in February 2014, and licenses for Formality by June 2014. As evidenced by the conduct discussed below, Tsai's statements on September 30, 2013 were false when made, and Tsai never intended to license the software from Synopsys as represented. Instead, as described in the piracy plan referenced in paragraphs 83-103 below, Tsai only intended to acquire a few "legal licenses" from an EDA vendor and pirate the rest of the software needed for the project.

52. On October 1, 2013, acting on behalf of the Piracy Enterprise, Tsai emailed Synopsys in Mountain View and represented that Ubiquiti had elected to take a Local Area Network ("LAN") form of Synopsys' licenses because the licenses would be used by a small U.S. team. Tsai stated "I don't think it's necessary for us to have the flexibility of checking out licenses across [different physical] sites over [a Wide Area Network]." As evidenced by the conduct discussed below, this statement was false when made, as Tsai, Pera, UNIL, and Ubiquiti always contemplated using Synopsys' software at numerous geographically distributed locations ranging from the Northern District of California to Taiwan. In fact, Tsai emailed Pera specifically to report on the concept of Synopsys' global WAN rights.

53. On October 14, 2013, acting on behalf of the Piracy Enterprise, Tsai emailed Synopsys in Mountain View and represented that Tsai intended for Ubiquiti to consummate its

first EDA tool purchase from Synopsys before October 31, 2013. Later that day in a subsequent email, Tsai told Synopsys via communications directed to Mountain View that Ubiquiti's preference would be to pay Synopsys from an "offshore account" in Hong Kong. As evidenced by the conduct below, this representation was false when made.

54. Also on October 14, 2013, acting on behalf of the Piracy Enterprise, Tsai emailed Synopsys in Mountain View and requested an evaluation license for Synopsys' VCS application. Tsai expressly represented that he would be "the one doing the eval" on his own personal laptop. Tsai further represented that he knew how to use VCS. Tsai's statements were false when made: in fact, Tsai intended all along for the evaluation to be done by other persons in Taiwan on computers that did not belong to Tsai.

55. On October 15, 2013, Tsai and Yang, via the interstate wires and computers used in interstate commerce, acting on behalf of the Piracy Enterprise, discussed a plan whereby Ubiquiti and UNIL would "use piracy" to "save some money." Tsai and Yang agreed that Ubiquiti and UNIL would purchase "at least a few legal licenses" but would supplement those legal licenses with pirated software and counterfeit keys in order to increase the AME team's capacity. Tsai explained to Yang that Ubiquiti and UNIL needed to move quickly.

56. Tsai's statements to Yang about the Piracy Enterprise's plans to purchase a few legal licenses were consistent with a pattern and practice by Ubiquiti, UNIL, and the Piracy Enterprise to conceal illegal activity by taking superficial measures designed to create the false appearance of legality with respect to the AME Project.

57. On October 15, 2013, Tsai traveled to Taipei where, acting on behalf of the Piracy Enterprise, he continued to represent that Ubiquiti was considering licensing Synopsys' EDA software while omitting material facts known to Tsai that were necessary to render his representations regarding Ubiquiti's intent non-misleading throughout. In reliance on Tsai's representations and omissions, Synopsys entered into a Master Non-Disclosure Agreement ("MNDA") with Ubiquiti, the purpose of which was to facilitate the parties' discussion of a potential business relationship. Ubiquiti and Synopsys executed the MNDA on October 15, 2013 and November 25, 2013, respectively.

58. Throughout the course of his negotiations with EDA providers in the U.S. and Taiwan, Tsai regularly reported to Pera, including via interstate wires and computers used in interstate commerce, regarding license terms, product costs, and the conduct of negotiations with Synopsys and other EDA providers.

59. From October 14, 2013 to November 25, 2013 Tsai, acting on behalf of the Piracy Enterprise, continued to represent that Ubiquiti was interested in licensing Synopsys' EDA tools. Throughout this period, Tsai and other Piracy Enterprise members and conspirators continued to discuss plans for pirating EDA software in order to reduce Ubiquiti and UNIL's development costs, which they believed would result in profits for the company and themselves. For example, on November 6, 2013, Tsai and Yang discussed technical means that could be used to exponentially increase the number of computers running EDA software without valid license keys. Such conduct was intended to and did reduce Ubiquiti and UNIL's development costs and development time. Members of the Piracy Enterprise also discussed anticipated raises if they delivered their contemplated ASIC on time, and they subsequently received these anticipated raises from Ubiquiti and UNIL notwithstanding Ubiquiti and UNIL's knowledge of the piracy conduct discussed herein.

60. Tsai ultimately negotiated an evaluation agreement under which Ubiquiti would, according to Tsai, evaluate Synopsys' VCS application at a specific Ubiquiti location in San Jose, California for a period not to exceed ninety days. During these negotiations, Tsai omitted that the Piracy Enterprise would in fact use counterfeit license keys and pirated copies of Synopsys' VCS application at unauthorized locations on unauthorized computers.

61. Tsai's representations to Synopsys in September, October, and November regarding Ubiquiti's desire to explore licensing Synopsys' products and willingness to conform to Synopsys' licensing terms were false when made. Shortly after fraudulently inducing Synopsys to grant Ubiquiti an evaluation license for Synopsys' VCS application—before the term of the evaluation license had even expired—persons acting on behalf of the Piracy Enterprise began using counterfeit license keys to access unauthorized copies of VCS from unauthorized locations. On information and belief, as soon as Tsai obtained access to Synopsys' file download and

customer support websites, the Piracy Enterprise began making and distributing unauthorized copies of Synopsys' software and documentation, accessing Synopsys' software using both illicit license key files and counterfeit facsimiles of Synopsys' license key files, and providing to one another software and other technology components designed to circumvent Synopsys' technical measures that control access to Synopsys' copyright-protected works.

62. In reliance on Tsai's representations and omissions, on November 26, 2013, Synopsys executed a 90-day evaluation license to permit Ubiquiti to evaluate Synopsys' VCS application. Synopsys sent to Tsai a delivery email containing links to download VCS and a license key for VCS. The license provided that it was a nontransferable limited evaluation license to use Synopsys' VCS application and the accompanying license key on two computers concurrently in San Jose. The evaluation license strictly proscribed limited evaluation rights and expressly prohibited any use of the software for designing Ubiquiti's products. The evaluation license also prohibited Ubiquiti from making unauthorized copies of Synopsys' software, decompiling or reverse engineering Synopsys' software, tampering with or attempting to circumvent Synopsys' license key system, or distributing Synopsys' software to third parties, among other restrictions. The evaluation license also contained a confidentiality clause prohibiting Ubiquiti from unauthorized dissemination or use of Synopsys' confidential information, defined to include *inter alia* Synopsys' software. The evaluation license contained a clause expressly stating that the evaluation license superseded all prior agreements between the parties regarding the subject matter of the evaluation license. The evaluation agreement provided that licensees consented to personal jurisdiction in federal and state courts of Santa Clara County, California.

63. In order to facilitate the evaluation license, and in reliance on Tsai's representations and omissions, Synopsys provided Tsai with temporary login credentials permitting Ubiquiti to access Synopsys' customer support and file download websites for purposes of facilitating Ubiquiti's evaluation of VCS. The Synopsys customer support and file download websites accessed by the Piracy Enterprise are all located on domains owned, registered, hosted, and maintained in the United States and the Northern District of California,

with the exception of one host server located in Ireland that the Piracy Enterprise accessed via a remote host located at Synopsys' Mountain View headquarters.

64. On November 27, 2013, Tsai, acting on behalf of the Piracy Enterprise, accessed Synopsys' file download website and downloaded multiple files, including Synopsys' VCS application, Synopsys' SCL license management application, installer programs for each application, and related documentation. The software downloaded by Tsai was hosted by Synopsys on, and downloaded from, servers located in the United States, including servers located within the State of California.

65. On November 28, 2013, Tsai, acting on behalf of the Piracy Enterprise, communicated via the interstate wires and computers used in interstate commerce instructions to a UNIL employee instructing him: "don't talk about cracking software using company email." Tsai explained that the risks of being caught pirating software were high because Ubiquiti is a publically traded company.

66. On December 2, 2013, Tsai, acting on behalf of the Piracy Enterprise, emailed Synopsys in Mountain View and stated that he was having trouble running Synopsys' license management software and temporary key file, purportedly on a virtual machine running on a computer located at Ubiquiti's San Jose headquarters. Synopsys customer support personnel responded to Tsai's inquiry and provided information on how to configure the license key file. Also on December 2, 2013, Tsai, acting on behalf of the Piracy Enterprise, emailed a Synopsys employee in Mountain View and requested for Synopsys to temporarily switch the Host ID listed in Ubiquiti's temporary key file to a new computer because, according to Tsai, the prior Host ID information he had provided was for an old personal laptop.

67. On information and belief, Tsai's December 2, 2013 representations were false when made. In fact, the purpose of Tsai's communication was to gain the information and means required by the Piracy Enterprise to carry out its purpose of running Synopsys' software on unauthorized computers in unauthorized locations. Tsai omitted these facts from his representations to Synopsys.

68. On December 4, 2013, Tsai and other members of the Piracy Enterprise discussed

with a UNIL employee, via interstate wires and computers used in interstate commerce, the costs of Synopsys products and "alternatives" to paying for the number of licenses needed to lawfully run "massive regressions" on "many computers."

69. Throughout the time period from November 27, 2013 to December 28, 2013, while Ubiquiti, UNIL, and other members of the Piracy Enterprise were actively engaged in the copying, creation, distribution, and use of counterfeit software, counterfeit license keys, and other circumvention technology, Tsai and one or more UNIL employees, acting on behalf of the Piracy Enterprise, accessed Synopsys' file download website and downloaded multiple files, including Synopsys' VCS application, Synopsys' SCL license management application, installer programs for each application, and related documentation. The software downloaded by Tsai, Ubiquiti, and UNIL was hosted by Synopsys on, and downloaded from, servers located in the United States, including servers located within the State of California.

70. On information and belief, throughout late 2013 and early 2014, Tsai and others acting on behalf of the Piracy Enterprise transferred via Ubiquiti and UNIL's shared IT infrastructure, the interstate wires, and computers used in interstate commerce some or all of the files downloaded from Synopsys to one or more computers controlled by UNIL.

71. In or about mid-December, 2013, Tsai, UNIL employees Andre Lee, Josh Huang, and/or other members of the Piracy Enterprise traveled to the United States with computers used in interstate commerce that, on information and belief, contained pirated software and/or counterfeit license keys for products belonging to multiple U.S. EDA companies.

72. On or about January 1, 2014, Tsai, UNIL employee I-Feng, and Ubiquiti employee Sheng-Feng Wang traveled to Ubiquiti's Barrington, Illinois research laboratory with computers used in interstate commerce that, on information and belief, contained pirated software and/or counterfeit license keys for products belonging to multiple U.S. EDA companies.

73. In or about January 2014, Tsai and other members of the Piracy Enterprise discussed, via the interstate wires and computers used in interstate commerce, use of pirated software tools to develop Ubiquiti's airFiber 5xHD product.

74. As discussed above, throughout pendency of the AME Project, Pera was actively

and intimately involved in hiring, procurement, and project management decisions related to the project. Pera hired all of the members of the AME Project Team. Tsai reported directly to Pera and provided regular updates on budgeting, software tools, and development issues. Tsai could not effect more than $2,000 in expenditures on the project without Pera's approval. Pera personally participated in software license meetings and negotiation and ultimately approved Ubiquiti and UNIL's bare-bones EDA software licensing plans, which facilitated the Piracy Enterprise's fraud and piracy, including piracy of tools for which Ubiquiti acquired a small number of licenses. On information and belief, Pera personally approved the purchase by UNIL of the Taiwan server array responsible for facilitating much of the piracy at issue in this case. This server array was specifically purchased to facilitate the AME Project's ASIC work and was one of the Piracy Enterprise's most prolific piracy instruments.

UNIL and Tsai Gain Further Access to Synopsys' Intellectual Property

75. During the first and second weeks of March 2014, Tsai, while physically located in the Northern District of California at Ubiquiti's headquarters and acting on behalf of the Piracy Enterprise, communicated with Synopsys via email about UNIL's purported desire to evaluate certain Synopsys software. Also included in these email discussions were other UNIL employees who work in the field of semiconductor design. Tsai emailed a quote he obtained under false pretenses from Synopsys in the fall of 2013 as the starting point for negotiations about obtaining a set of temporary evaluation license keys for UNIL. Tsai indicated that UNIL was close to obtaining software from a Synopsys competitor and wanted to evaluate Synopsys' competing tools before making a final decision. On information and belief, Tsai and other UNIL employees knew at the time of these email communications, but omitted to tell Synopsys, that UNIL had no intention of licensing Synopsys' software, but rather intended to make and distribute unauthorized copies of Synopsys' software and documentation and to use counterfeit license keys to circumvent Synopsys' license key system.

76. During the first and second weeks of April 2014, Tsai, acting on behalf of the Piracy Enterprise, traveled to Taiwan and helped coordinate a meeting between UNIL and Synopsys to discuss UNIL's purported desire to evaluate and license Synopsys' software. At

least Tsai and other UNIL employees attended a meeting with Synopsys on or about April 8, 2014, during which Tsai and others, acting on behalf of the Piracy Enterprise, represented to Synopsys through affirmative misrepresentations and omissions that access to temporary evaluation license keys for Synopsys' software could sway UNIL to license Synopsys' EDA tools. Tsai represented that time was of the essence due to the state of negotiations between UNIL and Synopsys' competitor and UNIL's time frame for completing design of the product for which the subject EDA tools were needed.

77. On information and belief, Tsai's representations to Synopsys in March and April 2014 regarding UNIL's purported consideration of licensing Synopsys' EDA products were false when made. At the time of such representations, UNIL and Ubiquiti employees were already making, distributing, and using unauthorized copies of Synopsys' software and documentation, circumvention technology, counterfeit license keys, and counterfeit access devices. Tsai omitted these material facts during his conversations with Synopsys.

78. In reliance on Tsai's representations, on April 14, 15, and May 9, 2014, Synopsys provided to UNIL temporary license keys for Synopsys' Formality, DC Ultra, HDL Compiler Verilog, and DesignWare Library applications. Also on May 9, 2014, Synopsys provided UNIL with a temporary key for its Power Compiler application. All of the temporary keys Synopsys provided to UNIL allowed for only one or two concurrently running executions, and all keys were designated to be hosted by license servers running only on specific computers with Host IDs enumerated in the temporary license key files that accompanied Synopsys' software. In addition, the temporary keys expired within two to four weeks after issuance.

79. On April 16, 2014, UNIL, acting on behalf of the Piracy Enterprise, downloaded Synopsys' license control software, its Formality and Design Compiler applications, and related documentation and installer files from Synopsys' electronic file transfer website. UNIL downloaded additional files on May 19, 2014. The files UNIL downloaded on April 16, 2014 were hosted on, and downloaded from, servers located in the United States, including servers located within the Northern District of California. With respect to the files downloaded on May 19, the files were downloaded via a remote host located at Synopsys' Mountain View

headquarters.

80. On April 16 and April 17, 2014, despite being in possession of temporary license keys for Design Compiler, UNIL employees acting on behalf of the Piracy Enterprise began using counterfeit license keys to access Design Compiler software downloaded by UNIL.

81. On May 19, 2014, a UNIL employee acting on behalf of the Piracy Enterprise contacted Synopsys' customer support via email for assistance in using tools that, unbeknownst to Synopsys, were secretly being copied and used without authorization by the Piracy Enterprise. The person who made this request on behalf of UNIL represented to Synopsys that time was of the essence, and that finding a quick solution to the subject issue could cause UNIL to license Synopsys' tool instead of licensing a competitor's tool. On information and belief, these statements were false when made, and the UNIL employee omitted material facts from their representation, including the fact of UNIL's true intent and its ongoing piracy conduct. In reliance on UNIL's representations and omissions, Synopsys customer support personnel in Mountain View communicated with UNIL and Ubiquiti regarding the issue and assisted in resolving the service request, which involved identifying and sharing with persons acting on behalf of the Piracy Enterprise a work-around solution to their problem and required an appreciable amount of effort and Synopsys resources. But for UNIL and Tsai's false representations and omissions regarding UNIL's purported desire to license Synopsys products, Synopsys would not have provided UNIL or Ubiquiti with the requested assistance or work-around information.

82. Subsequent to May 19, 2014, Tsai, UNIL, Ubiquiti, and other persons acting on behalf of the Piracy Enterprise repeatedly accessed Synopsys' customer support and file download websites. As soon as Synopsys issued temporary evaluation license keys to UNIL in April 2014, UNIL, Tsai, Ubiquiti, and others acting on behalf of the Piracy Enterprise began making, distributing, and using copies of Synopsys' software and documentation without authorization, including software and documentation downloaded from Synopsys servers located in the United States and California, and using counterfeit license keys and illicit license keys to access Synopsys' applications.

Conduct of the Piracy Enterprise

83. The volume and nature of counterfeit keys used by the Piracy Enterprise, including components of the counterfeit keys identifying specific computers controlled by UNIL and Ubiquiti, respectively, indicate that one or more persons acting on behalf of the Piracy Enterprise used counterfeit key generation software to create counterfeit Synopsys license keys for use by Ubiquiti and UNIL.

84. The nature of the counterfeit keys used by the Piracy Enterprise and use patterns for the infringed software applications indicate that members of the Piracy Enterprise distributed amongst themselves counterfeit license keys and/or counterfeit key generation software in order to permit employees of Ubiquiti and UNIL to access Synopsys' software without authorization. On information and belief, counterfeit keys and counterfeit key generation software was exchanged between members of the Piracy Enterprise using the Internet and Ubiquiti and UNIL's shared IT infrastructure.

85. Data associated with the Piracy Enterprise's use of Synopsys' software indicates that the Piracy Enterprise set up networks of computers that permitted persons to remotely access counterfeit keys, counterfeit key generation software, and unauthorized and counterfeit copies of Synopsys' software from multiple workstations connected to the Internet and to shared IT infrastructure via IP addresses, domains, and subdomains owned and/or controlled by Ubiquiti and UNIL.

86. Sometimes, the Piracy Enterprise configured computers to operate in "license server" mode, in which case a host server containing counterfeit license key files and running unauthorized copies of Synopsys' license management software could distribute counterfeit keys over the Internet to multiple remote computers.

87. Other times, the Piracy Enterprise employed a "serverless" configuration in which case the Piracy Enterprise would store counterfeit license key files at specific file paths located on Ubiquiti and UNIL networks for retrieval by any computer with access to the file path.

88. Other times, the Piracy Enterprise configured computers so that Synopsys' applications and counterfeit license keys were accessible from a virtual machine that, on

information and belief, could be accessed remotely and/or transported and used in and outside of California. Evidence indicates that the Piracy Enterprise used certain virtual machines in both California and in Taiwan.

89. Using at least the methods described above, the Piracy Enterprise distributed and used counterfeit license keys, illicit license keys, counterfeit access devices, and circumvention technology to access more than a dozen copyright protected works including Synopsys' Debussy, Design Compiler, Formality, HSPICE, IC Compiler, Laker, Nlint, nWave, PrimeTime, Synplify Pro AV, Synplify Premier AV, TetraMAX, VCS, and Verdi applications, among other EDA software titles, among other EDA software titles.

90. The Piracy Enterprise's counterfeit license key use is associated with at least fifteen distinct usernames, most of which correspond to the names of known Ubiquiti and UNIL employees such as Tsai, Lian, Yang, Wang, Huang, Feng, Hau-Lin Hsu, and Chang-Ching Yang.

91. Synopsys conducted an investigation into whether Ubiquiti was using counterfeit license keys to access Synopsys' software that culminated in a May 2016 notice to Ubiquiti demanding that it cease and desist unauthorized use of Synopsys' software. Notwithstanding this communication, the Piracy Enterprise continued to access unauthorized copies of Synopsys' software using counterfeit keys until at least December 2017—nearly a year after Synopsys filed the instant action in U.S. District Court. Synopsys did not and could not know of this continued piracy because the Piracy Enterprise reconfigured their firewalls to block call-home signals to Synopsys in order to continue their unlawful scheme undetected.

Ubiquiti and UNIL's Failure to Investigate and Complicity in the Piracy Enterprise

92. Synopsys' May 2016 notice to Ubiquiti warned of impending legal action, including escalation to formal legal proceedings against Ubiquiti for *inter alia* copyright infringement. In addition, the notice advised Ubiquiti of its duty to "PRESERVE DIGITAL EVIDENCE, as required by law." Both Pera and Ubiquiti's Vice President of Legal Affairs received Synopsys' infringement notice, but neither of them took steps to preserve digital evidence or conducted a reasonable investigation into Synopsys' allegations. This failure to preserve evidence and failure to promptly investigate violated the Ubiquiti Code of Business

Conduct and Ethics. On information and belief, the Ubiquiti Audit Committee has not investigated these executive-level omissions.

93. After receiving the May 2016 notice, Ubiquiti's Vice President of Legal Affairs, via interstate wires and computers used in interstate commerce, forwarded the notice to only Tsai. Tsai then forwarded the Vice President of Legal Affairs' email to Piracy Enterprise members and UNIL employees James Lian, Andre Lee, and Josh Huang, each of whom used counterfeit keys to access Synopsys' software, and instructed them not to discuss the issue over email. Subsequent to receiving this email, Tsai, Lee, Huang, and Lian each took steps to conceal and destroy evidence of their conduct.

94. In violation of Ubiquiti corporate policy, Pera, some or all members of Ubiquiti Management, and other Ubiquiti and UNIL executives willfully turned a blind eye to the rapacious fraud and piracy occurring at Ubiquiti and UNIL, which they knew or had reason to know was occurring. No one at Ubiquiti or UNIL undertook diligent efforts to investigate Synopsys' allegations or prevent further piracy. *Inter alia*, Ubiquiti and UNIL failed to conduct interviews of relevant employees, failed to instruct employees to preserve evidence, failed to quarantine the accused UNIL server environment that Ubiquiti Management and UNIL executives knew or reasonably should have known was used to host Synopsys' software, failed to inspect employee computers or review employee emails, and failed to instruct its employees regarding the alleged copyright infringement.

95. On information and belief, Pera and/or one or more of members of Ubiquiti Management approved the purchase of the UNIL infrastructure used to host the AME Project team's EDA software tools and work product, including three computational servers purchased for the express purpose of running large ASIC design jobs, and these individuals thus knew that the Taiwan server array was the objectively obvious place to look for evidence related to Synopsys' allegations. Yet despite having the authority and technical means to remotely inspect these critical evidentiary sources, Ubiquiti and UNIL leadership failed to investigate their employees' misconduct and failed to preserve material evidence. The result of Ubiquiti and UNIL's failure to act was continued violations of federal law by the Piracy Enterprise and its

members, followed by spoliation of evidence.

96. Neither Ubiquiti nor UNIL's responsible personnel promptly reported Synopsys' allegations to Ubiquiti's Audit Committee. On information and belief, the Piracy Enterprise's pattern of misconduct, especially as rampant and unchecked as it was, would have a material impact on the Company's financial performance and should have been reported to the Audit Committee so that appropriate disclosures could be made and measures could be taken.

97. Ubiquiti, via interstate wires and computers used in interstate commerce, knowingly or in the alternative recklessly made false statements to Synopsys designed to mislead Synopsys about the scope of Ubiquiti's conduct. For example, Ubiquiti represented to Synopsys that U.S.-based Ubiquiti employee Sheng-Feng Wang could not have possibly used Synopsys software because Wang did not have access to the tools. In fact, Wang had local copies on his personal devices of unauthorized Synopsys software and counterfeit license keys, in addition to having remote access to UNIL owned servers in Taiwan that Defendants concede were used to host Synopsys' software. These are facts that Ubiquiti and UNIL either knew were false or would have easily discovered to be false through even a cursory investigation. Ubiquiti and UNIL's knowing or reckless misrepresentations demonstrate complicity with the Piracy Enterprise. Ubiquiti and UNIL were willfully blind to the facts that made these representations false.

98. After receiving word of Synopsys' infringement notice, Tsai, acting on behalf of the Piracy Enterprise, instructed UNIL and Ubiquiti on how to reconfigure their computing environments to prevent Synopsys and other EDA software owners from detecting Defendants' piracy. Tsai and other members of the Piracy Enterprise also undertook to destroy log files and other digital evidence of their piracy activities. All told, Defendants spent over 140 person hours attempting to delete evidence and block Synopsys call-home software from reporting violations.

99. Subsequent to Synopsys' infringement notice and according to verified discovery responses, Pera traveled to Taiwan and met with the AME Project Team, specifically, on information and belief, Tsai, Lian, Yang, Wang, Huang, Feng, Hau-Lin Hsu, and Chang-Ching Yang, and/or other members of the Piracy Enterprise. During this meeting, Pera purportedly talked about the importance of respecting intellectual property. But at the conclusion of his

remarks, Pera stated that anyone *caught* using licensed software in the future would be immediately terminated. The message that Pera conveyed, and that the Piracy Enterprise members clearly received, was that no discipline would come to those careful enough to avoid detection (either by the software owners or willfully blind Ubiquiti and UNIL executives). Notably, after Ubiquiti Management informed Tsai that Synopsys reported the AME Project piracy, Tsai and others reconfigured Ubiquiti's and UNIL's systems so that they could continue using Synopsys' tools while avoiding detection by Synopsys. To date, Defendants have produced no evidence showing that Ubiquiti or UNIL ever instructed the AME Project Team to cease and desist using unlicensed Synopsys' software.

100. Subsequent to Pera's Piracy Enterprise meeting, members of the Piracy Enterprise continued to use pirated Synopsys software (and other companies' pirated software) to perform work for UNIL and Ubiquiti—this time, however, they took extra measures to avoid detection by Synopsys, including obfuscation and destruction of digital evidence. Piracy Enterprise members ultimately received raises for their work on the AME Project; Pera authorized these raises *after* Synopsys filed this case shedding light on Ubiquiti's and UNIL's wide scale piracy.

101. From May 10, 2016 through at least December 2017 (just before court-ordered forensic inspections were set to commence), members of the Piracy Enterprise continued to pirate Synopsys software in furtherance of their work for Ubiquiti and UNIL.

102. Throughout 2016 and 2017, Tsai and other Ubiquiti and UNIL employees, acting on behalf of the Piracy Enterprise, continued to use Synopsys' pirated software to develop an ASIC for the Ubiquiti airFiber 5xHD. Ubiquiti commenced manufacturing of the airFiber 5xHD containing the ASIC designed by the Piracy Enterprise in 2017. Ubiquiti is currently importing the airFiber 5xHD from manufacturing facilities in China into the United States and is distributing the airFiber 5xHD in interstate commerce throughout the United States, including by means of interstate wires, interstate mail, and computers used in interstate commerce.

103. According to Defendants' verified discovery responses, Ubiquiti conducted an "investigation" of Synopsys' allegations that commenced in May 2016 and ended on or about February 28, 2018. This "investigation," if it happened at all, was a sham designed to create the

false appearance of legality. Tellingly, despite purportedly investigating Synopsys' allegations for nearly two years, Ubiquiti and UNIL failed to gather any material evidence (which was readily available), and the only remedial action Ubiquiti and UNIL took was to send a February 28, 2018 email to UNIL and Ubiquiti employees "reminding" them to use company equipment and software in a proper manner. This email, too, was a sham designed to create the false appearance of legality and to pay lip service to the company policies prohibiting use of unlicensed or pirated software.

104. Defendants' verified discovery responses establish that Ubiquiti and UNIL executive leadership were at best complicit in the ongoing illegal conduct carried out by the Piracy Enterprise from May 2016 to early 2018; at worst, they knowingly and actively participated in the Piracy Enterprise's conduct. If it is true that Ubiquiti and UNIL undertook a diligent investigation that lasted nearly two years, they undoubtedly uncovered internal company emails evidencing piracy of Synopsys software and other EDA software but failed to act to remedy past piracy and prevent such piracy from continuing to occur. If they had conducted a diligent investigation, Ubiquiti and UNIL would have found illegal EDA software and license keys on company property, but they either failed to preserve the evidence their investigation produced or destroyed it.

105. Alternatively, if Ubiquiti and UNIL conducted any investigation at all, it was a sham investigation designed to avoid finding relevant evidence. On information and belief, to the extent Ubiquiti and UNIL made any efforts at all to investigate Synopsys' allegations, the goal of the investigation was to facilitate a cover up and permit Ubiquiti and UNIL to maintain the appearance of plausible deniability.

106. As of the date of this filing, not a single Ubiquiti or UNIL employee has been actually disciplined for unlicensed use of Synopsys software. Nor has any Ubiquiti or UNIL employee been disciplined for the rampant spoliation of evidence Synopsys has uncovered. Indeed Tsai and key members of the AME Project Team have received raises authorized by Pera himself.

Defendants' Spoliation and Obstruction of Justice

107. Ubiquiti and UNIL contacted Morrison & Foerster in response to Synopsys' allegations at least as early as July 2016. Despite the fact that Ubiquiti and UNIL clearly anticipated the prospect of litigation, Ubiquiti Management and/or UNIL executives intentionally or recklessly failed to supervise and direct outside counsel to ensure proper collection and preservation of evidence. Among other objectively reckless acts and omissions by Ubiquiti and UNIL prior to February 2017:

- Ubiquiti and UNIL did not advise outside counsel of where to look for relevant evidence, or alternatively, did advise outside counsel of where to look for relevant evidence but failed to ensure that outside counsel collected evidence from such sources or actively prevented outside counsel from collecting from such sources;
- Neither Ubiquiti, UNIL, nor any of their counsel instructed Ubiquiti or UNIL employees to preserve and not destroy documents and other digital evidence until sometime in, at the earliest, February 2017, nine months after Ubiquiti was notified of its duty to preserve evidence;
- Neither Ubiquiti, UNIL, nor any of their counsel inspected employee computers or company servers for unlawful software or counterfeiting tools;
- Neither Ubiquiti, UNIL, nor any of their counsel inspected or collected evidence from critical devices and storage locations that obviously contained relevant evidence;
- Ubiquiti, UNIL, and/or their counsel permitted Ubiquiti and/or UNIL employees known to have engaged in culpable conduct to self-collect their own documents, resulting in the permanent loss of material evidence.

108. During Ubiquiti and UNIL's period of inaction, the Piracy Enterprise continued to pirate software belonging to Synopsys and others and continued to destroy evidence.

109. Even after Synopsys filed suit on February 3, 2017, Ubiquiti Management and UNIL executives failed to conduct any serious investigation into the federal crimes being carried out by Ubiquiti and UNIL employees. These omissions were due in part to pressure on Pera from the Ubiquiti Board of Directors and others who were expressing concerns that the AME Project

was not a "real project." Pera and other executives at Ubiquiti and UNIL knew that a diligent investigation into the AME Project's use of EDA software would reveal serious and ongoing violations of law, and that such a revelation would require Pera, pursuant to Ubiquiti corporate policy, to terminate nearly the entire AME team, thereby jeopardizing the time to market for Ubiquiti's airFiber 5xHD product and negatively impacting the company's financial performance. Moreover, in a 2017 earnings call with investors, Pera touted his successful recruitment of the Tsai AME ASIC team and did not want the piracy conduct of his prized AME Project and ASIC design team to become public. Pera and others at Ubiquiti and UNIL therefore made the conscious decision not to investigate Synopsys' allegations and, on information and belief, resolved to take an obstructionist, lackadaisical approach to collecting evidence that would allow Ubiquiti and UNIL to maintain plausible deniability until after the airFiber 5xHD's release.

110. Synopsys served its first set of requests for production of documents and tangible things from Defendants on May 12, 2017. On information and belief, Ubiquiti and UNIL failed to supervise and direct its outside counsel to ensure that a reasonable and diligent search for responsive information was collected, reviewed, and produced in a timely manner. *Inter alia*, Ubiquiti and UNIL failed to ensure that outside counsel collected documents from relevant shared file repositories and failed to ensure that digital evidence on Ubiquiti and UNIL employee computers was preserved. As a result of Ubiquiti's failure, relevant evidence was permanently lost or destroyed.

111. Had Defendants conducted a timely, reasonable and diligent search of relevant computers, communications, and document repositories after receiving Synopsys' document requests, Defendants would have discovered ongoing piracy and the existence of Synopsys' software and communications on Ubiquiti and UNIL devices.

112. On information and belief, sometime in mid to late 2017, Ubiquiti and UNIL's outside counsel discovered internal Ubiquiti and UNIL emails discussing (1) unlicensed use of Synopsys' software and efforts by Tsai and others to ensure that their continued software piracy would not be detected by Synopsys or other EDA providers; and (2) Defendants' practice of making copies of virtual machines containing Synopsys' EDA software and distributing those

virtual machine copies for local installation on Ubiquiti and UNIL employee laptops, including laptops running Windows operating systems. On information and belief, Ubiquiti and UNIL's outside counsel communicated these findings to at least Ubiquiti Vice President of Legal Affairs, who instructs outside counsel on the conduct of this case. Yet Ubiquiti and UNIL failed to direct and supervise outside counsel to ensure collection of relevant evidence, including on Ubiquiti and UNIL employee laptops.

113. On September 8, 2017, Synopsys served a formal forensic inspection request identifying various UNIL and Ubiquiti computers by MAC address, known IP addresses, and usernames. Despite their obligations under federal law, Ubiquiti and UNIL failed to supervise and direct its outside counsel to ensure that these devices were collected and preserved. Instead, Ubiquiti Management and UNIL executives permitted the technically skilled perpetrators of a massive, high value software piracy scheme to maintain possession of material digital evidence comprising computers, hard drives, and servers used to host and run Synopsys software. As of the date of this filing, Ubiquiti and UNIL's outside counsel have still not completed collection and imaging of relevant devices. Even more troubling, Ubiquiti and UNIL either did not permit or did not instruct outside counsel to begin collecting devices from most UNIL employees until *March 2018*—over a year after this litigation commenced and months after the Court advised Defendants that the devices were relevant to discovery. Massive spoliation predictably resulted from Ubiquiti's and UNIL's intentional delay in collecting material evidence.

114. Because Ubiquiti and UNIL refused to preserve or produce the Piracy Enterprise computers, Synopsys was required to seek a Court order compelling (1) forensic inspection of laptops and other devices belonging to the UNIL and Ubiquiti employees implicated by Synopsys' allegations, and (2) a live inspection of Ubiquiti and UNIL server environment in Taiwan. In an attempt to convince U.S. Magistrate Judge Beeler that inspection of Ubiquiti and UNIL employee laptops should not be granted, Ubiquiti and UNIL represented on multiple occasions, including in false sworn declarations submitted to the Court, that none of Defendants' employees ever installed Synopsys's EDA tools on their laptop devices. In a hearing before Judge Beeler on January 25, 2018, Ubiquiti and UNIL told the Court through counsel that:

"[Synopsys] software does not operate on a Windows environment or on a Mac environment. So there is no reason they need to look at any of the individual computers that use Mac and Windows as their operating environment." Yet at the time these representations were made to the Court, Ubiquiti and UNIL already knew that employees had installed Synopsys tools on laptops running Windows and Mac operating systems, because (1) Ubiquiti and UNIL already knew from outside counsel's document review of emails discussing installation of Synopsys tools on virtual machines contained on employee laptops; and (2) Ubiquiti and UNIL already knew from outside counsel's forensic inspection that Tsai's Windows-based laptop exhibited evidence of the presence of virtual machines and Synopsys tools (in addition to evidence of spoliation).

115. In an order issued on December 22, 2017, U.S. Magistrate Judge Laurel Beeler indicated that the computers Synopsys sought were likely to have relevant evidence and ordered Defendants to meet and confer with Synopsys regarding an inspection protocol. Despite Judge Beeler's guidance in December 2017, Ubiquiti and UNIL failed to supervise and direct their outside counsel to ensure that digital evidence on the subject devices would be preserved for Synopsys' inspection. On the contrary, Defendants intentionally delayed collection and preservation of the subject devices for months. All the while, Ubiquiti and UNIL employees, acting on behalf of the Piracy Enterprise, were actively spoliating evidence.

116. Ubiquiti and UNIL executive leadership disregarded the objectively obvious risk that their failure to supervise and direct counsel to collect and preserve digital evidence would result in the permanent loss of evidence relevant to an ongoing official proceeding in U.S. District Court. Indeed, on information and belief, after outside counsel engaged Epiq Systems ("Epiq") to image some (but not all) of Defendant Tsai's devices in November 2017, outside counsel learned that Tsai used a memory wiping tool to permanently destroy evidence of Ubiquiti and UNIL's software piracy from his devices shortly before turning the devices over to Epiq, and outside counsel communicated this finding to at least some Ubiquiti Management and UNIL executives. Nevertheless, Ubiquiti Management and UNIL executives turned a blind eye to this spoliation of evidence and delayed collecting and preserving other relevant employee devices for nearly four months. Further spoliation predictably resulted from this protracted, intentional delay.

117. Despite having known of the impending court-ordered forensic inspection since December 2017, and despite having constructive and actual notice of spoliation by Tsai and Wang as of January 2018, Ubiquiti and UNIL failed to supervise and direct outside counsel to take the steps necessary to preserve evidence subject to the Court's inspection order. Instead, Ubiquiti and UNIL permitted outside counsel to delay collection of the subject devices and then provided the Piracy Enterprise's members with advance notice of device collection times, abetting further spoliation.

118. During at least the time period between May 2016 and mid-March 2018, Ubiquiti employees including Tsai and Wang and UNIL employees Lian, Huang, Yang, and/or other members of the Piracy Enterprise engaged in a pattern of deleting, destroying, altering, and tampering with evidence of piracy of Synopsys' software. Ubiquiti and UNIL employees used the same or similar deletion and obfuscation techniques and deletion tools, and deletions appeared to have been phased to coincide with Epiq's phased collection efforts. In some instances, deletions occurred minutes before Epiq commenced imaging.

119. During a court-ordered native server inspection of the Piracy Enterprise's primary computational server array in Taiwan, Ubiquiti and UNIL obstructed Synopsys' forensic examiner's execution of Judge Beeler's inspection order. Ubiquiti and UNIL were particularly recalcitrant with respect to Synopsys' attempt to inspect unallocated memory space on the servers—which is where remnants of deleted evidence would reside. As a result of Ubiquiti and UNIL's conduct, Synopsys' forensic examiners were forced to sit idle in Taiwan for nearly a week while Ubiquiti and UNIL permitted known spoliators to access the subject servers. By the time Synopsys' forensic experts (FTI) finally gained Court-ordered access to search unallocated space on Defendants servers (after an emergency discovery hearing before Judge Beeler), most unallocated space on the devices had been completely overwritten. Nevertheless, deleted evidence of use of Synopsys software remained and was recovered from unallocated space in the Taiwan server array.

120. Forensic discovery remains ongoing, including with respect to newly discovered devices belonging to Tsai that neither Ubiquiti/UNIL's outside counsel nor Tsai's personal

counsel made any effort to collect and produce until their existence was discovered during Tsai's April 15, 2018 deposition. The existence of these additional devices was known, or should have been known, to defendants as a result of the forensic inspections completed by the date of Tsai's deposition.

121. Although much evidence has been permanently destroyed, a clear pattern of deliberate, calculated, and coordinated spoliation has emerged. Among other findings, inspection of Ubiquiti and UNIL employees' devices has revealed that:

a. Days before Tsai's work-issued computers and external hard drive were imaged for inspection in November 2017, Tsai deleted and overwrote numerous files and folders, including those that appear to have contained Synopsys materials. Tsai used a software program called CCleaner to permanently destroy evidence on his computer.

b. Days before Ubiquiti employee Sheng-Feng Wang's work-issued devices were imaged in January 2018, Wang overwrote his external hard drive memory with hundreds of duplicate copies of a few large video files, preventing recovery of data previously stored on the drive. In addition, Wang's computer contained virtual machines that appeared to contain deleted Synopsys-related files and evidence that deletion commands had been used.

c. Approximately 15 minutes before his device was imaged in March 2018, UNIL employee Chi-Hsueh Huang ran CCleaner twice in rapid succession.

d. UNIL employee James Lian's external hard drive contained Synopsys files in the Recycle Bin and a folder containing Synopsys-related files that had been deleted days before the device was imaged in December 2017. Lian's other devices showed evidence of deletion commands and wiping.

e. UNIL employee Ya-Chau Yang deleted virtual machine files from his computer and then used a "shredder" wiping tool to permanently overwrite the deleted data. Additionally, Yang's computer showed evidence consistent with use of the CCleaner data wiping utility which caused permanent destruction of hundreds of

files.

f. UNIL employee Yi-Te Lee deleted files and then copied data numerous times in order to overwrite the deleted files; this activity happened on similar days that Tsai deleted and wiped data (i.e., a few days prior to the collection of Tsai's devices).

g. UNIL employee Chang-Ching Yang's computer showed evidence that Yang used the data wiping utility CCleaner to permanently destroy 5,000 files less than two days prior to the collection of Yang's devices in March 2018.

h. UNIL employee Hua-Lin Hsu's computer showed evidence of suspicious deletion of a number of files in February, 2017, shortly after the lawsuit was filed. Hsu's computer also showed that Hsu deleted Google chat and Skype chat data from his computer in February 2018 shortly before his computer was collected for inspection; remnants of this deleted data indicate that Hsu used chat services to discuss Synopsys products at issue in this case.

i. After an emergency hearing in which Judge Beeler ordered Defendants to cooperate with FTI's attempts to search for deleted evidence in unallocated space on Ubiquiti and UNIL's Taiwan servers, FTI located evidence of commands used to specifically search out and delete Synopsys software along with evidence of commands used to erase the command log history file on the servers in Taiwan; although much evidence had been permanently destroyed by the time FTI gained access to Defendants servers, some remnants of deleted evidence remained in unallocated space at the time of inspection in March 2018 and showed that Defendants continued to use Synopsys software well *after* this lawsuit commenced.

122. On information and belief, Tsai, Ubiquiti, UNIL and other members of the Piracy Enterprise each encouraged and assisted the other to commit the violations of law discussed herein by inducing each other to gain unauthorized access to Synopsys' software, to use and traffic counterfeit license keys, illicit license keys, circumvention technology, and counterfeit access devices, to destroy evidence, and by providing their services to assist each other in doing

so.

123. Before the forensic evidence was obtained, Tsai provided sworn answers to interrogatories and made sworn declarations that were filed with this Court. At his deposition, taken after much of the forensic evidence had been discovered, Tsai refused to testify about virtually all of the matters at issue in this case by invoking his Fifth Amendment privilege against self-incrimination. Additional devices were disclosed during Tsai's deposition. Those devices are currently being examined for further forensic evidence of piracy, conspiracy, spoliation and obstruction of justice.

FIRST CLAIM FOR RELIEF

(Against All Defendants for Violation of the

Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)(1))

124. Synopsys hereby restates and re-alleges the allegations set forth in paragraphs 1 through 123 above and incorporates them by reference.

125. Section 1201(a)(1) provides, in pertinent part, that no person shall circumvent a technological measure that effectively controls access to a work protected under title 17.

126. Synopsys' EDA software, including its Debussy, Design Compiler, Formality, HSPICE, IC Compiler, Laker, Nlint, nWave, PrimeTime, Synplify Pro AV, Synplify Premier AV, TetraMAX, VCS, and Verdi applications, is subject to protection under the copyright laws of the United States.

127. Access to Synopsys' EDA software, including its Debussy, Design Compiler, Formality, HSPICE, IC Compiler, Laker, Nlint, nWave, PrimeTime, Synplify Pro AV, Synplify Premier AV, TetraMAX, VCS, and Verdi applications, is controlled by technological measures: namely, the Synopsys License Key system.

128. Rather than paying a license to Synopsys for access and use of the EDA software, the Piracy Enterprise used counterfeit license keys that Tsai, Ubiquiti, and UNIL knew to be counterfeit and in violation of Synopsys' valuable rights.

129. By using counterfeit license keys, Tsai, Ubiquiti, and UNIL have circumvented the Synopsys License Key access-control system, and have unlawfully gained access thereby to at

least its Debussy, Design Compiler, Formality, HSPICE, IC Compiler, Laker, Nlint, nWave, PrimeTime, Synplify Pro AV, Synplify Premier AV, TetraMAX, VCS, and Verdi copyright protected software applications.

130. Tsai, Ubiquiti, UNIL, and other members of the Piracy Enterprise agreed to act in concert in order to gain access to Synopsys' software and documentation and to circumvent technological measures that effectively control access to Synopsys' works. Subsequent to this agreement, one or more members of the Piracy Enterprise committed wrongful acts in furtherance of the agreement.

131. The conduct described above has caused harm to Synopsys in an amount to be computed at trial, but that amount is in the millions of dollars and constitutes a violation of 17 U.S.C. § 1201. Synopsys is entitled to remedies including statutory damages, actual damages, and any profits attributable to Defendants' violations.

132. The conduct described above was willful and with knowledge of wrongdoing; an award of maximum statutory damages is therefore necessary to dissuade Defendants and others from the use of counterfeit license keys.

133. Accordingly, pursuant to 17 U.S.C. § 1203, Synopsys is entitled to and hereby demands statutory damages in the maximum amount of $2,500 for each of the violations of the statute.

134. Synopsys is further entitled to an award of attorneys' fees and costs as provided under 17 U.S.C. § 1203.

SECOND CLAIM FOR RELIEF

(Against All Defendants for Violations of the

Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)(2))

135. Synopsys hereby restates and re-alleges the allegations set forth in paragraphs 1 through 134 above and incorporates them by reference.

136. Section 1201(a)(2) provides, in pertinent part, that no person shall manufacture, import, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof that is primarily designed or produced for the purpose of circumventing a

technological measure that effectively controls access to a work protected under title 17.

137. Tsai, Ubiquiti, and UNIL created, imported, provided, or trafficked in products, services, or components or parts thereof primarily designed and produced for the purpose of circumventing technological measures that effectively control access to Synopsys' works.

138. Tsai, Ubiquiti, UNIL, and others members of the Piracy Enterprise agreed to act in concert in order to create, import, provide, or traffic in products, services, or components or parts thereof primarily designed and produced for the purpose of circumventing technological measures that effectively control access to Synopsys' works. Subsequent to this agreement, one or more members of the Piracy Enterprise committed wrongful acts in furtherance of the agreement.

139. The conduct described above has caused harm to Synopsys in an amount to be computed at trial, but that amount is in the millions of dollars and constitutes a violation of 17 U.S.C. § 1201. Synopsys is entitled to remedies including statutory damages, actual damages, and any profits attributable to Defendants' violations.

140. The conduct described above was willful and with knowledge of wrongdoing; an award of statutory damages is necessary to dissuade Defendants and others from the use of counterfeit license keys.

141. Accordingly, pursuant to 17 U.S.C. § 1203, Synopsys is entitled to and hereby demands statutory damages in the maximum amount of $2,500 for each of the violations of the statute.

142. Synopsys is further entitled to an award of attorneys' fees and costs as provided under 17 U.S.C. § 1203.

THIRD CLAIM FOR RELIEF

(Against All Defendants for Violations of the

Digital Millennium Copyright Act, 17 U.S.C. § 1201(b))

143. Synopsys hereby restates and re-alleges the allegations set forth in paragraphs 1 through 142 above and incorporates them by reference.

144. Section 1201(b) provides, in pertinent part, that no person shall manufacture, import, provide, or otherwise traffic in any technology, product, service, device, component, or

part thereof that is primarily designed or produced for the purpose of circumventing a technological measure that effectively protects a right of an owner of a work protected under title 17.

145. Tsai, Ubiquiti, and UNIL created, imported, provided, or trafficked in products, services, or components or parts thereof primarily designed and produced for the purpose of circumventing technological measures that effectively protect Synopsys' rights in its works.

146. Tsai, Ubiquiti, UNIL, and other members of the Piracy Enterprise agreed to act in concert in order to create, import, provide, or traffic in products, services, or components and parts thereof primarily designed and produced for the purpose of circumventing technological measures that effectively protect Synopsys' rights. Subsequent to this agreement, one or more members of the Piracy Enterprise committed wrongful acts in furtherance of the agreement.

147. The conduct described above has caused harm to Synopsys in an amount to be computed at trial, but that amount is in the millions of dollars and constitutes a violation of 17 U.S.C. § 1201. Synopsys is entitled to remedies including statutory damages, actual damages, and any profits attributable to Defendants' violations. The conduct described above was willful and with knowledge of wrongdoing; an award of statutory damages is necessary to dissuade Defendants and others from the use of counterfeit license keys.

148. Accordingly, pursuant to 17 U.S.C. § 1203, Synopsys is entitled to and hereby demands statutory damages in the maximum amount of $2,500 for each of the violations of the statute.

149. Synopsys is further entitled to an award of attorneys' fees and costs as provided under 17 U.S.C. § 1203.

FOURTH CLAIM FOR RELIEF

(Against All Defendants for Violations of 18 U.S.C. § 2318)

150. Synopsys hereby restates and re-alleges the allegations set forth in paragraphs 1 through 149 above and incorporates them by reference.

151. Section 18 U.S.C § 2318 provides in pertinent part that it is a federal crime for persons to knowingly traffic in counterfeit or illicit labels accompanying a copy of a computer

program. Any copyright owner who is injured, or is threatened with injury, by a violation of subsection section 2318 may bring a civil action in an appropriate United States district court.

152. Synopsys delivers authorized copies of its copyright protected software to licensees over the Internet via a secured file transfer protocol in binary form. In order to access Synopsys binaries, licensees must validate their copies of Synopsys' software with license keys that accompany the customer's specific authorized copies of Synopsys' software. Synopsys license keys are designed to ensure that users do not designate a higher number of licensed users or licensed copies than authorized and to prevent infringement.

Synopsys' License Keys Are Software Identifying Labels

153. Synopsys' license key files are identifying labels accompanying and designed to accompany copies of Synopsys' computer programs. The counterfeit keys used by Defendants mimicked the human readable text elements and format of Synopsys' genuine keys, including texts suggesting that Synopsys is the issuer of the keys. Synopsys license key files are comprised of human readable alphanumeric text elements that identify the name, version, and features of the Synopsys software licensed by the specific license key recipient. Synopsys license keys also identify Synopsys as the owner of the software and issuer of the license key. Synopsys license keys also identify the name and address of the licensee of the software that the license key accompanies. Synopsys license keys also identify a customer Site ID and host server designated by the licensee to run Synopsys' software. Synopsys license keys also direct licensees to follow the license file verification procedure set forth at http://www.synopsys.com/licensing when installing or updating the licensee's license file and advise licensees that their license key must be verified with Synopsys' verification utility. Synopsys license verification utility confirms that license keys are valid to authorize execution of the software licensed to the licensee. Synopsys license key files further identify the date and time on which the license key file was created and the start and end date of the included license keys. The identifying information contained in Synopsys license keys (in addition to messages contained in license key transmittal emails and/or the pages of Synopsys download websites) indicates to the recipient that the license key is being delivered in connection with a specific software product configured to run features licensed by a

specific customer.

154. When a user launches a Synopsys EDA application, Synopsys SCL software begins to execute and locates the directory where the licensee has saved her license key file or determines how to access the Synopsys license server. After retrieving the license key from either the license file or from the server, the SCL software displays to the user the server host, site ID, and license term dates set forth in the license key. After SCL identifies the correct license key, the EDA application begins to execute. The EDA application user interface displays to the user the name of the EDA application (i.e., "Design Compiler"), software version (i.e., Version 1.2.3), and operating system that the application is written for (i.e., 64-bit Linux). The application user interface further displays to the user trademark information for the application that is being run. The application user interface then displays a copyright notice that provides, for example, "Copyright (c) 1988-2017 Synopsys, Inc. This software and the associated documentation may only be used in accordance with the terms and conditions of a written license agreement with Synopsys, Inc. All other use, reproduction, or distribution of this software is strictly prohibited." Where applicable, the application user interface then displays to the user the various distinct features of the application that have been specifically licensed by the particular licensee. Finally, after validating each specifically licensed feature against the license key, the application user interface displays to the user a message stating that the license key checkout has succeeded. The user may then use the application to perform EDA functions.

155. Where a user lacks a valid license key, Synopsys SCL software detects the lack of a valid key and will not complete execution. Similarly, the EDA application itself cannot execute because no license key is served to it. The EDA application user interface displays a message to the user indicating that the wrong license file is being used and instructing the user to contact Synopsys.

156. As noted, one of the identifying aspects of Synopsys license keys is identification of the specific features that a licensee has licensed. Synopsys' EDA applications contain a wide array of rich features, some of which may not be necessary for a customer's specific design project. For example, a customer designing a simple electronic circuit may not require all of the

latest, most advanced features of a given Synopsys EDA application. Thus, rather than paying for a license to unneeded features, customers may license a subset of the total feature set for a given Synopsys EDA application. Synopsys license keys identify the subset of licensed features, and an engineer who wishes to identify which features are available to her can look to the license key file for that information. For each copy of an authorized Synopsys EDA application binary, the accompanying Synopsys license keys reflects the unique feature set licensed by a particular licensee, which dictates the scope of how the particular copy of the licensed binary will execute. Unlicensed features not validated by the customer's license key will not run. In this way, Synopsys license keys identify and define the licensee's unique configuration of the Synopsys software they have licensed.

Synopsys' License Keys Verify that a Software Copy is Not Counterfeit or Infringing

157. Synopsys license key files, including temporary evaluation license key files, are genuine licensing and labeling components used by Synopsys to verify that a copy of a computer program is not counterfeit or infringing of any copyright, and to prevent parties from providing Synopsys' software to a higher number of licensed users than authorized.

158. Because Synopsys only provides genuine, authorized copies of its software to licensees, and because license keys always accompany Synopsys' delivery of its software, Synopsys license keys are used by Synopsys to verify that a copy of a computer program is not counterfeit or infringing. When a user runs an unauthorized copy of Synopsys' software using a counterfeit license key, Synopsys can determine whether it or an unauthorized third party was the source of the copy of the software executed with the counterfeit license key. For example, in this case, Ubiquiti and UNIL used counterfeit license keys to run applications that they did not download from Synopsys' file transfer websites. Synopsys' license key system helped Synopsys identify the copies of these applications used by Ubiquiti and UNIL as unauthorized counterfeit copies provided by unknown third parties.

159. Synopsys license keys also prevent licensees from providing Synopsys' software concurrently to a higher number of licensed users than authorized under the terms of the applicable license. Once a license key has been checked out to a user, that checkout is counted

against the total number of concurrent instances of the application that the licensee is authorized to run under the terms of their license. For example, if a user's license permits three concurrent uses of Design Compiler, only two additional users would be permitted to run Design Compiler after a first user executes Design Compiler. If a fourth user attempts to execute Design Compiler while three other users already have license keys checked out, Synopsys' license key system detects the fact that the maximum number of concurrent users set forth in the license key file has already been checked out, and the fourth user's attempt to run the application will fail.

160. On information and belief, Ubiquiti knowingly trafficked in illicit labels by providing to UNIL unauthorized copies of Synopsys' software and temporary license keys issued for Ubiquiti's Mountain View location to UNIL. The copies of Synopsys EDA applications that UNIL executed using the temporary license keys issued to Ubiquiti were unauthorized copies.

161. On information and belief, UNIL knowingly trafficked in illicit labels by providing unauthorized copies of Synopsys' software and temporary license keys issued for UNIL's Taiwan location to Ubiquiti. The copies of Synopsys EDA applications that Ubiquiti executed using these temporary license keys issued to UNIL were unauthorized copies.

162. Tsai, Ubiquiti, and UNIL knowingly trafficked in counterfeit license key files that appeared to be genuine, but were not. The counterfeit license keys trafficked by Defendants mimicked the human readable text, structure, and format of Synopsys genuine license keys and would appear to an innocent reader of the key file to be a genuine Synopsys license key.

163. Tsai, Ubiquiti, and UNIL intentionally used counterfeit and illicit labels in connection with trafficking in goods or services.

164. Tsai, Ubiquiti, and UNIL knowingly and intentionally trafficked in counterfeit license keys likely to cause confusion, to cause mistake, or to deceive persons not privy to the Piracy Enterprise. For example, on information and belief, based on representations made by counsel and Ubiquiti to this Court, at least one employee of Ubiquiti and/or UNIL was unaware that the software copies and license keys he used to perform EDA services for Ubiquiti and/or UNIL in California were counterfeit. According to a May 1, 2017 declaration submitted to this Court (Dkt. 50-1), at least for a time, California-based Ubiquiti employee Sheng-Feng Wang was

not aware that he had received any unauthorized license keys or copies of Synopsys license keys in California. Sheng-Feng Wang's declaration indicates the counterfeit license keys and software copies used by the Piracy Enterprise were capable of being, and on information and belief, were in fact, passed off to unsuspecting end users as genuine license keys.

165. In carrying out their violations of 18 U.S.C § 2318, Tsai, Ubiquiti, and UNIL used and intended to use facilities of interstate and foreign commerce.

166. Counterfeit and illicit labels trafficked and used by Tsai, Ubiquiti, and UNIL accompanied, were enclosed with, or affixed to, or were designed to accompany, be affixed to, or enclosed with, copyrighted copies of computer programs.

167. Tsai, Ubiquiti, UNIL, and other members of the Piracy Enterprise agreed to act in concert in order to traffic or use counterfeit license key files and illicit license key files. Subsequent to this agreement, one or more members of the Piracy Enterprise committed wrongful acts in furtherance of the agreement.

168. The conduct described above has caused harm to Synopsys in an amount to be computed at trial. Synopsys is entitled to actual damages and any profits attributable to Defendants' violations.

169. The conduct described above was willful and with knowledge of wrongdoing; an award of statutory damages is necessary to dissuade Defendants and others from the use of counterfeit license keys.

170. Accordingly, pursuant to 18 U.S.C. § 2318, Synopsys is entitled to and hereby demands statutory damages in the maximum amount of $25,000 for each of the violations of the statute.

FIFTH CLAIM FOR RELIEF

(Against All Defendants for Fraud)

171. Synopsys hereby restates and re-alleges the allegations set forth in paragraphs 1 through 170 above and incorporates them by reference.

172. Tsai, acting on behalf of the Piracy Enterprise, knowingly made false representations of material fact to Synopsys during the time period between October and

December 2013 in order to induce Synopsys to grant Tsai access to Synopsys' file download and customer support websites, and to grant Ubiquiti an evaluation license for VCS. Tsai also omitted material facts necessary to render his representations non-misleading. Specifically, acting on behalf of the Piracy Enterprise:

i. Tsai falsely represented that Ubiquiti was interested in evaluating, negotiating, and licensing Synopsys' software in good faith;

ii. Tsai falsely represented that Ubiquiti intended to evaluate VCS in San Jose, California;

iii. Tsai falsely represented that he needed assistance with setting up Synopsys' software and temporary license keys for legitimate use in San Jose;

iv. Tsai omitted that Ubiquiti and UNIL would make and use unauthorized copies of Synopsys' software and documentation;

v. Tsai omitted that he would provide his login credentials and/or Synopsys materials accessed through such credentials to unauthorized persons including UNIL employees in Taiwan;

vi. Tsai omitted that Ubiquiti and UNIL would use circumvention technology, counterfeit license keys, and illicit license keys to access Synopsys' software without authorization.

173. Tsai and others at UNIL, acting on behalf of the Piracy Enterprise, knowingly made false representations of material fact to Synopsys during April and May 2014 in order to induce Synopsys to grant UNIL temporary evaluation license keys and access to Synopsys' file download and customer support websites. Tsai also omitted material facts necessary to render his representations non-misleading. Specifically, acting on behalf of the Piracy Enterprise:

i. Tsai falsely represented that UNIL was interested in evaluating, negotiating, and licensing Synopsys' software in good faith;

ii. Tsai falsely represented that time was of the essence as UNIL was close to signing a deal with a Synopsys competitor;

iii. Tsai or another UNIL employee falsely represented to Synopsys customer support

on May 19, 2014 that if Synopsys could develop a work around solution for a problem UNIL was having with Synopsys' tools, the work around could convince UNIL to license Synopsys' tools rather than a competitor's tools;

iv. Tsai omitted that UNIL would make and use unauthorized copies of Synopsys' software and documentation;

v. Tsai omitted that UNIL had already been using and would continue to use circumvention technology, counterfeit license keys, and illicit license keys to access Synopsys' software without authorization;

174. As to each of the above representations and omissions, Tsai, Ubiquiti, UNIL, and other members of the Piracy Enterprise intended for Synopsys to rely on the false representations and omissions.

175. Synopsys reasonably relied on Tsai's and the Piracy Enterprise's false representations and omissions. Synopsys had no reason to know of the Piracy Enterprise's true intent.

176. Synopsys relied on Tsai's and the Piracy Enterprise's false representations in granting Tsai access to Synopsys' file download and customer support websites, executing an evaluation license for Ubiquiti, and issuing temporary evaluation license keys to Ubiquiti and UNIL.

177. The Piracy Enterprise agreed to act in concert in order to gain access to Synopsys websites, software, documentation, and services using material misrepresentations and omissions communicated to Synopsys and to use circumvention technology and counterfeit and illicit licenses to access Synopsys' works. Subsequent to this agreement, one or more members of the Piracy Enterprise committed wrongful acts in furtherance of the agreement.

178. Synopsys' reliance on Tsai's and the Piracy Enterprise's representations caused Synopsys harm in an amount to be proven at trial.

179. The conduct described above was willful and with knowledge of wrongdoing; an award of punitive damages is necessary to dissuade Defendants and others.

SIXTH CLAIM FOR RELIEF

(Against All Defendants for Civil RICO, 18 U.S.C. § 1964(c) & (d))

180. Synopsys hereby restates and re-alleges the allegations set forth in paragraphs 1 through 179 above and incorporates them by reference.

181. Section 1962(c) provides that is unlawful for any person employed by or associated with any enterprise engaged in interstate or foreign commerce to conduct such enterprise's affairs through a pattern of racketeering activity.

182. Section 1962(d) provides that is unlawful for any person to conspire to violate section 1962.

183. Section 1964(c) provides that a person injured in their business or property by a violation of section 1962 may sue to recover threefold damages and the cost of suit, including reasonable attorney's fees.

The Enterprises

184. Ubiquiti is an enterprise organized under the laws of Delaware that affects interstate commerce.

185. UNIL is an enterprise organized under the laws of Hong Kong that affects interstate commerce.

186. The Piracy Enterprise is an ongoing association in fact that affects interstate commerce whose members functioned as a continuing unit for the common purpose of achieving the objectives of the Piracy Enterprise, including enriching the members and associates of the Piracy Enterprise through copyright infringement, trafficking and using counterfeit and illicit labels, trafficking and using counterfeit access devices, and destroying evidence of the foregoing in an attempt to obstruct justice. Members of the Piracy Enterprise include at least Tsai, Wang, Lian, Yang, Huang, Ubiquiti, and UNIL.

Conduct of the Enterprises

187. Tsai and others at Ubiquiti and UNIL are associated in fact and have conducted Ubiquiti and UNIL's affairs through a coordinated and continuous pattern of illegal activity for the common purpose of pirating Synopsys' software in order to lower Ubiquiti and UNIL's

semiconductor development costs, reap ill-gotten profits, and to cover up evidence of their crimes.

188. Ubiquiti and UNIL each provided funding, infrastructure, employee resources, and logistical support needed to conduct the Piracy Enterprise. Through Pera and/or Tsai, Ubiquiti and UNIL controlled and directed Defendants' employees and members of the scheme, who were managed by and reported to Tsai and Pera. Under Pera's direction and control, Tsai was responsible for negotiating with third party EDA software providers to gain for UNIL and Ubiquiti access to EDA tools necessary to carry out their scheme. As alleged above, at all times, Defendants acted under the control and direction of Tsai and/or Pera, whose approval was given to purchase EDA tools and who participated in meetings with software vendors, handled and approved of pricing and oversaw Tsai's efforts to obtain EDA tools for use by Ubiquiti and UNIL.

189. As alleged above, Ubiquiti Management and UNIL executives facilitated and further enabled the Piracy Enterprise by failing to maintain (or enforce) adequate internal controls to prevent unauthorized use of intellectual property by the AME Project Team and by recklessly or intentionally permitting deletion of digital evidence. For example, Ubiquiti apparently lacked any internal process for verifying that its employees were using properly licensed software. Only after Synopsys notified Ubiquiti of the infringement did Ubiquiti purport to take remedial measures such as admonishing Ubiquiti and UNIL employees about the importance of respecting intellectual property. Even then, Ubiquiti did not halt the piracy or discipline or terminate anyone for their piracy. Indeed, it rewarded them.

190. At the very least, Ubiquiti, UNIL, and their executive management were willfully blind to the fact that the Piracy Enterprise engaged in illegal conduct, particularly after Synopsys' May 2016 notice.

191. Tsai, Ubiquiti, UNIL, and others have conducted and participated in the affairs of the Piracy Enterprise through a pattern of racketeering activity that affects interstate and foreign commerce. The Piracy Enterprise and its members have committed numerous predicate acts as set forth below.

192. On information and belief, in or about October 2013, Tsai, Ubiquiti, and UNIL, conspired to operate Ubiquiti, UNIL, and the Piracy Enterprise through a pattern of racketeering activity in furtherance of the common purpose of the Piracy Enterprise, including achievement of the objectives of the AME Project. Tsai, Ubiquiti, and UNIL each took wrongful acts in furtherance of their unlawful agreement by financing and/or managing the Piracy Enterprise, attempting to gain and gaining access to Synopsys' software and documentation, making and distributing unauthorized copies of Synopsys' software and documentation, making, using, and distributing counterfeit and illicit license keys and counterfeit access devices to access Synopsys copyright protected software, instructing UNIL employees on how to hack MAC addresses in order to exponentially increase the number of concurrent software copies they could run, and destroying evidence, among other wrongful acts in furtherance of the Piracy Enterprise. Tsai, Ubiquiti, and UNIL continuously and effectively carried out the purpose of the Piracy Enterprise from at least October 2013 to mid-March 2018, causing harm to Synopsys in the form of at least but not limited to misappropriation of valuable intellectual property, lost licensing revenue, and costs associated with remediating Defendants' conduct.

193. On October 15, 2013, Tsai and Yang, via the interstate wires and computers used in interstate commerce, acting on behalf of the Piracy Enterprise, discussed a plan whereby Ubiquiti and UNIL would "use piracy" to "save some money." Tsai and Yang agreed that Ubiquiti and UNIL would purchase "at least a few legal licenses" but would supplement those legal license with pirated software and counterfeit keys in order to increase the AME team's capacity. Tsai explained to Yang that Ubiquiti and UNIL needed to move quickly. Then Tsai and Yang made opaque references to being escorted out of the office by police along with an unidentified "general counsel" and "VP of legal affairs."

194. From October 14, 2013 to November 25, 2013 Tsai, acting on behalf of the Piracy Enterprise, continued to represent that Ubiquiti was interested in licensing Synopsys' EDA tools. Throughout this period, Tsai and other Piracy Enterprise conspirators continued to discuss plans for pirating EDA software in order to reduce Ubiquiti and UNIL's development costs, which they believed would result in profits for the company and themselves. For example, on November 6,

2013, Tsai and Yang discussed technical means that could be used to exponentially increase the number of computers running EDA software without valid license keys. Such conduct was intended to and did reduce Ubiquiti and UNIL's development costs and development time. Members of the Piracy Enterprise also discussed anticipated raises if they delivered their contemplated ASIC on time, and they subsequently received these anticipated raises from Ubiquiti and UNIL notwithstanding Ubiquiti and UNIL's knowledge of the piracy conduct discussed herein.

Pattern of Racketeering

195. At all times relevant, Tsai, Ubiquiti, UNIL, and other members of the Piracy Enterprise knew that they did not have a valid license, permission, authorization, or other authority from Synopsys to use its copyright-protected software and documentation.

196. Tsai, Ubiquiti, UNIL and other members of the Piracy Enterprise violated 17 U.S.C. § 506 on multiple occasions by knowingly and willfully infringing for the purpose of financial gain copyright-protected works owned by Synopsys.

197. Tsai, Ubiquiti, UNIL and other members of the Piracy Enterprise violated 18 U.S.C § 1343 by using telephones, the Internet, and email communication in furtherance of a fraudulent scheme to gain access to Synopsys' intellectual property by deceiving Synopsys about Ubiquiti and UNIL's purported intent to license Synopsys' software. On at least October 14 and December 2, 2013, Tsai misrepresented and omitted material facts in email communications with Synopsys that were intended to induce Synopsys to provide Ubiquiti and UNIL with access to valuable intellectual property belonging to Synopsys.

198. Tsai, Ubiquiti, UNIL and other members of the Piracy Enterprise violated 18 U.S.C § 2318 on multiple occasions by knowingly trafficking in and using counterfeit labels.

199. On information and belief, Tsai, Ubiquiti, UNIL and other members of the Piracy Enterprise have violated 18 U.S.C § 2318 on multiple occasions by knowingly trafficking in and using illicit labels.

200. Tsai, Ubiquiti, UNIL and other members of the Piracy Enterprise have violated 18 U.S.C. § 1029 on multiple occasions by knowingly and with the intent to defraud: (i) using and

trafficking in counterfeit access devices to obtain access to valuable software, the value of the use of which aggregates more than $1,000 per one-year period; (ii) possessing fifteen or more devices which are counterfeit or unauthorized access devices; and (iii) producing, trafficking, and having custody, possession, and control of counterfeit access device making equipment. By way of example and not limitation, the counterfeit license keys used by the Piracy Enterprise are counterfeit access devices. In addition, members of the Piracy Enterprise configured computers and virtual machines into counterfeit access devices in order to obfuscate and alter Host IDs, IP addresses, MAC addresses, and other identifying information so that the Piracy Enterprise could misrepresent the location and identity of devices containing Synopsys' software and gain unauthorized access to Synopsys' valuable intellectual property. The Piracy Enterprise trafficked in such access devices and used them to deprive Synopsys of millions of dollars in licensing fees.

201. In order to receive any software from Synopsys, a customer must first open up a customer account with Synopsys by registering for Synopsys' SolvNet website and entering into a license agreement. After establishing an account, customers may then submit purchase orders for the software they wish to license under their account for a given license term. This contractual relationship makes possible the provision of software and support services based on payment or expectation of payment at a later point in time to Synopsys. Absent compliance with the payment obligations of their account, customers are not authorized to use Synopsys' software. One type of Synopsys customer account is a fixed-term technology subscription license ("TSL") account in which a customer may license specific software for a specific term. Another type of Synopsys customer account is a flexible spending account ("FSA") with an assigned a dollar value against which the customer may draw down to apply to Variable Time-Based Technology Subscription Licenses ("VTSL"). For these types of customer accounts, for each request for a VTSL, the FSA balance is reduced by the applicable VTSL fee.

202. When a third party uses a counterfeit license key to run Synopsys software, they gain access to goods and services that they would otherwise not have access to without paying monies into a Synopsys customer account. Ubiquiti, for example, paid no monies into any FSA or other type of Synopsys customer account, yet accessed millions of dollars' worth of software

and services by using counterfeit access devices such as those described above. In essence, Defendants' counterfeit keys gave them access to an unlimited FSA to use against an all-encompassing technology pool. Alternatively, framed another way, Defendants' counterfeit license keys permit access to fictitious customer accounts with inordinately long TSLs so that they could access software without paying for it for many years.

203. On information and belief, Defendants have obtained unauthorized copies of Synopsys software from unknown third parties in the past and continue to have the know-how and capability to obtain more unauthorized Synopsys software from such sources.

204. On information and belief, prior to the events described in this lawsuit, Defendants used counterfeit license keys to access EDA tools from another software provider.

205. On information and belief, Ubiquiti and UNIL continue to employ persons with the know-how and ability to create counterfeit license keys.

206. In furtherance of the Piracy Enterprise, on multiple occasions between May 10, 2016 and mid-March 2018, Tsai, Ubiquiti, UNIL and other members of the Piracy Enterprise violated 18 U.S.C. §§ 1512(b)(2) by knowingly using intimidation, corruptly persuading, and/or engaging in misleading conduct with the intent to cause or induce others to (a) withhold records, documents, and other objects from an official proceeding; (b) alter, destroy, mutilate, or conceal objects and digital evidence contained thereon with the intent to impair the objects integrity or availability for use in an official proceeding; and/or (c) evade legal process summoning persons to produce records, documents or other objects in an official proceeding.

207. In furtherance of the Piracy Enterprise, on multiple occasions between May 10, 2016 and mid-March 2018, Tsai, Ubiquiti, UNIL and other members of the Piracy Enterprise violated 18 U.S.C. § 1512(c)(1) by corruptly altering, destroying, mutilating, and/or concealing records, documents, and other objects, and by attempting to do so, with the intent to impair the integrity or availability of same for use in an official proceeding.

208. The conduct described above has caused harm to Synopsys' business and property in an amount to be computed at trial.

209. The conduct described above was willful and with knowledge of wrongdoing.

210. Synopsys is entitled to and hereby demands treble damages, attorney's fees, and costs of suit.

SEVENTH CLAIM FOR RELIEF

(Against All Defendants for Negligent Misrepresentation)

211. Synopsys hereby restates and re-alleges the allegations set forth in paragraphs 1 through 210 above and incorporates them by reference.

212. The Piracy Enterprise agreed to act in concert in order to gain access to Synopsys websites, software, documentation, and services using material misrepresentations and omissions communicated to Synopsys and to use circumvention technology and counterfeit and illicit licenses to access Synopsys' works. Subsequent to this agreement, one or more members of the Piracy Enterprise committed wrongful acts in furtherance of the agreement.

213. Tsai, acting on behalf of the Piracy Enterprise, made material representations of fact to Synopsys that were untrue and omitted facts necessary to render his statements non-misleading.

214. Tsai had no reasonable grounds for believing his false representations were true.

215. Tsai intended for Synopsys to rely on his misrepresentations and omissions.

216. Synopsys reasonably relied on Tsai's representations.

Reliance on Tsai's false representations was a substantial factor in harm caused to Synopsys by Defendants.

PRAYER FOR RELIEF

WHEREFORE, Synopsys prays for judgment against Defendants as follows:

A. Entry of judgment in favor of Synopsys against Defendants;

B. An order awarding Synopsys statutory and/or actual damages and disgorgement of profits for each instance on which Defendants circumvented measures controlling access to Synopsys' software pursuant to 17 U.S.C. § 1203;

C. An order awarding Synopsys statutory and/or actual damages and disgorgement of profits for each instance on which Defendants provided circumvention technology pursuant to 17 U.S.C. § 1203;

D. An order awarding Synopsys statutory and/or actual damages and disgorgement of profits for each instance on which Defendants trafficked in counterfeit or illicit labels under 18 U.S.C. § 2318;

E. An order awarding Synopsys treble damages and attorney's fees under 18 U.S.C. § 1964;

F. An order awarding Synopsys actual damages and punitive damages for harm proximately caused by Defendants' fraud and/or negligent representation;

G. An order granting appropriate relief to Synopsys for Defendants' obstruction of justice, including but not limited to striking some or all of Defendants' pleadings, issuing preclusive sanctions on legal and/or evidentiary issues, and giving adverse inference instructions to the jury.

H. Prejudgment and post-judgment interest;

I. An order awarding Synopsys its costs and attorneys' fees pursuant to 17 U.S.C. § 1203;

J. An order for an accounting of all gains, profits, cost savings and advantages realized by Defendants from their acts;

K. Imposition of a constructive trust over all revenues generated by sales of products containing the ASIC designed by the Piracy Enterprise;

L. An order preliminarily and permanently enjoining Defendants, their officers, agents, servants, employees, attorneys, and affiliated companies, their assigns and successors in interest, and those persons in active concert or participation with them, from the statutory violations alleged herein; and

M. All such further and additional relief, in law or equity, to which Synopsys may be entitled or which the Court deems just and proper.

Dated: June 7, 2018

DENISE M. MINGRONE
ROBERT L. URIARTE
Orrick, Herrington & Sutcliffe LLP

By: */s/Denise M. Mingrone*
DENISE M. MINGRONE
Attorneys for Plaintiff
SYNOPSYS, INC.

DEMAND FOR A JURY TRIAL

Synopsys demands a jury trial for all issues so triable.

Dated: June 7, 2018

DENISE M. MINGRONE
ROBERT L. URIARTE
ORRICK, HERRINGTON & SUTCLIFFE LLP

By: */s/ Denise M. Mingrone*
DENISE M. MINGRONE
Attorneys for Plaintiff
SYNOPSYS, INC.